

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-143889

(43)Date of publication of application : 20.05.2004

(51)Int.Cl.

E05B 49/00  
B60R 25/00  
B60R 25/10  
G06K 17/00  
H04L 9/08  
H04L 9/32

(21)Application number : 2002-312807

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 28.10.2002

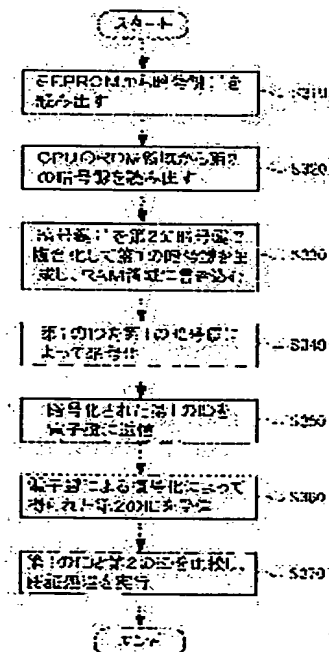
(72)Inventor : IKEDA KAZUYA

## (54) IN-VEHICLE INSIDE ELECTRONIC KEY DEVICE AND AUTHENTICATION METHOD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an in-vehicle electronic key device by making it difficult to forget an electronic key by acquiring a cipher key from an in-vehicle device, and to provide an authentication method.

**SOLUTION:** The in-vehicle electronic key device is provided with a step S310 for reading the cipher key to be ciphered obtained to cipher a first cipher key from a non-volatile memory; a step S320 for reading a second cipher key for decoding the cipher key to be ciphered and first discrimination information from an ROM region; a step S330 for storing to generate the first cipher key by using the second cipher key; a step S340 for ciphering the first discrimination information by using the first cipher key stored in an RAM region; a step S350 for transmitting the first ciphered discrimination information to an outside communication device; a step S360 for receiving a signal including second discrimination information stored by the outside communication device; and a step S370 for processing authentication by using the second discrimination information included in a received signal and the first discrimination information.



BEST AVAILABLE COPY

### LEGAL STATUS

[Date of request for examination] 29.09.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(19) 日本国特許庁(JP)

## (12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-143889

(P2004-143889A)

(43) 公開日 平成16年5月20日(2004.5.20)

(51) Int. Cl.<sup>7</sup>

E05B 49/00  
B60R 25/00  
B60R 25/10  
G06K 17/00  
H04L 9/08

F I

E05B 49/00 K  
B60R 25/00 606  
B60R 25/10 617  
G06K 17/00 T  
H04L 9/00 601A

テーマコード (参考)

2E250  
5B058  
5J104

審査請求 未請求 請求項の数 4 O L (全 8 頁) 最終頁に続く

(21) 出願番号 特願2002-312807(P2002-312807)  
(22) 出願日 平成14年10月28日(2002.10.28)

(71) 出願人 000005821  
松下電器産業株式会社  
大阪府門真市大字門真1006番地  
(74) 代理人 100072604  
弁理士 有我 軍一郎  
(72) 発明者 池田 和也  
神奈川県横浜市港北区綱島東四丁目3番1  
号 松下通信工業株式会社内  
Fターム(参考) 2E250 AA21 BB08 CC15 DD06 EE09  
FF27 FF36 HH01 JJ05 KK03  
LL01 TT03  
5B058 CA17 KA02 KA04 KA08 KA31  
KA35 YA11  
5J104 AA07 KA02 KA04 KA06 KA15  
NA37 NA38 PA15

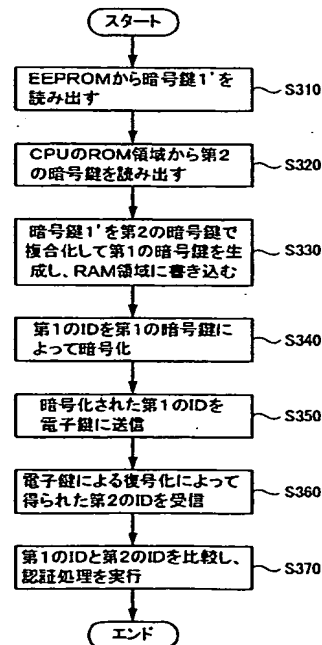
(54) 【発明の名称】 車載電子鍵装置および認証方法

## (57) 【要約】

【課題】 車載装置から暗号鍵を取得して電子鍵を偽造することを困難にするための車載電子鍵装置および認証方法を提供すること。

【解決手段】 第1の暗号鍵を暗号化して得られる被暗号化暗号鍵を不揮発性メモリから読み出すステップS310と、被暗号化暗号鍵を復号化するために用いる第2の暗号鍵および第1の識別情報をROM領域から読み出すステップS320と、第2の暗号鍵を用いて第1の暗号鍵を生成して記憶するステップS330と、RAM領域に記憶された第1の暗号鍵を用いて第1の識別情報を暗号化するステップS340と、暗号化した第1の識別情報を外部の通信装置に送信するステップS350と、外部の通信装置が記憶する第2の識別情報を含む信号を受信するステップS360と、受信した信号中に含まれる第2の識別情報と第1の識別情報とを用いて認証処理を行うステップS370と、を備えた構成を有している。

【選択図】 図3



## 【特許請求の範囲】

## 【請求項 1】

第 1 の暗号鍵を暗号化して得られる被暗号化暗号鍵を記憶する不揮発性メモリと、前記不揮発性メモリが記憶する前記被暗号化暗号鍵を復号化して前記第 1 の暗号鍵を生成するために用いる第 2 の暗号鍵を ROM 領域に記憶した演算処理部とを備え、作動が停止しても前記第 2 の暗号鍵の情報を保持する記憶領域であることを特徴とする車載電子鍵装置。

## 【請求項 2】

外部の通信装置と無線通信するための無線通信インタフェースを備え、前記演算処理部は、さらに認証処理に用いる第 1 の識別情報を ROM 領域に記憶し、作動時または作動後に前記第 2 の暗号鍵を用いて前記被暗号化暗号鍵を復号化して前記第 1 の暗号鍵を生成し、生成した前記第 1 の暗号鍵を RAM 領域に記憶し、前記 RAM 領域に記憶された第 1 の暗号鍵を用いて前記第 1 の識別情報を暗号化し、前記暗号化した前記第 1 の識別情報を前記無線通信インタフェース経由で前記外部の通信装置に送信し、前記外部の通信装置が記憶する第 2 の識別情報を含む信号を前記無線通信インタフェース経由で受信し、受信した前記信号中に含まれる前記第 2 の識別情報と前記第 1 の識別情報とを用いて認証処理を行い、前記 ROM 領域に記憶された前記第 1 の識別情報は、作動が停止しても情報が保持されることを特徴とする請求項 1 記載の車載電子鍵装置。

## 【請求項 3】

第 1 の暗号鍵を暗号化して得られる被暗号化暗号鍵を不揮発性メモリから読み出すステップと、前記被暗号化暗号鍵を復号化するために用いる第 2 の暗号鍵および第 1 の識別情報を ROM 領域から読み出すステップと、前記第 2 の暗号鍵を用いて前記被暗号化暗号鍵を復号化して前記第 1 の暗号鍵を生成し、生成した前記第 1 の暗号鍵を記憶するステップと、前記 RAM 領域に記憶された第 1 の暗号鍵を用いて前記第 1 の識別情報を暗号化するステップと、前記暗号化した前記第 1 の識別情報を外部の通信装置に送信するステップと、前記外部の通信装置が記憶する第 2 の識別情報を含む信号を受信するステップと、受信した前記信号中に含まれる前記第 2 の識別情報と前記第 1 の識別情報とを用いて認証処理を行うステップと、を備え、前記 ROM 領域に記憶された前記第 1 の暗号鍵および前記第 1 の識別情報は、作動が停止しても情報が保持されることを特徴とする認証方法。

## 【請求項 4】

前記第 2 の識別情報と前記第 1 の識別情報とを用いて行う処理認証は、前記第 2 の識別情報と前記第 1 の識別情報とが一致する場合に認証し、一致しない場合は認証しない請求項 3 記載の認証方法。

## 【発明の詳細な説明】

## 【0001】

## 【発明の属する技術分野】

本発明は、自動車等の盗難防止に用いられる車載電子鍵装置および認証方法に関する。

## 【0002】

## 【従来の技術】

従来、電子鍵と車載電子鍵装置を用いて行う盗難防止のための認証方法は、車載電子鍵装置と電子鍵とで識別情報（以下、ID という。）等の所定の情報を無線通信し、受信した信号から ID 等を抽出して認証を行い、ID が認証された場合にドアの施解錠を行うものであった（例えば、特許文献 1 参照。）。その際、車載電子鍵装置と電子鍵とは、車載電子鍵装置毎に異なる共通の暗号鍵を保有し、この暗号鍵を用いて暗号化および復号化を行い、ID の機密性を保持するようにしていた。

## 【0003】

ここで、従来の車載電子鍵装置では、車載電子鍵装置毎に異なる暗号鍵を、電子鍵内と車載電子鍵装置内の電氣的に書き込み及び消去が可能な不揮発性メモリとに記憶させていた。この不揮発性メモリとして、例えば EEPROM 等が用いられ、暗号鍵の記憶はもちろん、変更をも行うことができるようにするものであった。

## 【0004】

図4に、電子鍵と車載電子鍵装置を用いて行う従来の盗難防止のための認証方法における処理の流れを示すフローチャートを示す。

まず、不揮発性メモリから暗号鍵を読み出し（S410）、車載電子鍵装置が保持する第1のIDを暗号鍵により暗号化し（S420）、暗号された第1のIDを電子鍵に送信し（S430）、電子鍵によって復号化された第2のIDを受信し（S440）、受信した第2のIDと上記の第1のIDとを比較し、認証を行う（S450）。認証は、2つのIDが一致するか否かで行われ、一致した場合に施解錠が行われるものである。

【0005】

【特許文献1】

特開平8-170457号公報

【0006】

【発明が解決しようとする課題】

しかし、このような従来の車載電子鍵装置または認証方法では、内蔵する不揮発性メモリからデータを読み出すことが容易であり、読み出したデータから暗号鍵を推定し、暗号鍵を知ることにより暗号化方式を解読すること容易になり、偽造電子鍵を作成することが可能になるという問題点があった。

【0007】

本発明はこのような問題を解決するためになされたもので、車載装置から暗号鍵を取得して電子鍵を偽造することを困難にするための車載電子鍵装置および認証方法を提供するものである。

【0008】

【課題を解決するための手段】

本発明の車載電子鍵装置は、第1の暗号鍵を暗号化して得られる被暗号化暗号鍵を記憶する不揮発性メモリと、前記不揮発性メモリが記憶する前記被暗号化暗号鍵を復号化して前記第1の暗号鍵を生成するために用いる第2の暗号鍵をROM領域に記憶した演算処理部とを備え、作動が停止しても前記第2の暗号鍵の情報を保持する記憶領域である構成を有している。

この構成により、被暗号化暗号鍵を復号するための第2の暗号鍵がROM領域に記憶されているため、車載装置から暗号鍵を取得して電子鍵を偽造することを困難にすることが可能な車載電子鍵装置および認証方法を実現することができる。

【0009】

また、本発明の車載電子鍵装置は、外部の通信装置と無線通信するための無線通信インタフェースを備え、前記演算処理部は、さらに認証処理に用いる第1の識別情報をROM領域に記憶し、作動時または作動後に前記第2の暗号鍵を用いて前記被暗号化暗号鍵を復号化して前記第1の暗号鍵を生成し、生成した前記第1の暗号鍵をRAM領域に記憶し、前記RAM領域に記憶された第1の暗号鍵を用いて前記第1の識別情報を暗号化し、前記暗号化した前記第1の識別情報を前記無線通信インタフェース経由で前記外部の通信装置に送信し、前記外部の通信装置が記憶する第2の識別情報を含む信号を前記無線通信インタフェース経由で受信し、受信した前記信号中に含まれる前記第2の識別情報と前記第1の識別情報とを用いて認証処理を行い、前記ROM領域に記憶された前記第1の識別情報は、作動が停止しても情報が保持される構成を有している。

この構成により、被暗号化暗号鍵を復号するための第2の暗号鍵がROM領域に記憶されているため、車載装置から暗号鍵を取得して電子鍵を偽造することを困難にすることが可能であると共に、暗号化した暗号鍵を記憶し、それを復号化して使用する機能または処理を従来の装置に付加するものであるため、新たに付加するハードウェアやソフトウェア等を最小限に抑えることができるため、安価に安全性を飛躍的に向上させることが可能な車載電子鍵装置を実現することができる。

【0010】

また、本発明の認証方法は、第1の暗号鍵を暗号化して得られる被暗号化暗号鍵を不揮発性メモリから読み出すステップと、前記被暗号化暗号鍵を復号化するために用いる第2の

10

20

30

40

50

暗号鍵および第1の識別情報をROM領域から読み出すステップと、前記第2の暗号鍵を用いて前記被暗号化暗号鍵を復号化して前記第1の暗号鍵を生成し、生成した前記第1の暗号鍵を記憶するステップと、前記RAM領域に記憶された第1の暗号鍵を用いて前記第1の識別情報を暗号化するステップと、前記暗号化した前記第1の識別情報を外部の通信装置に送信するステップと、前記外部の通信装置が記憶する第2の識別情報を含む信号を受信するステップと、受信した前記信号中に含まれる前記第2の識別情報と前記第1の識別情報とを用いて認証処理を行なうステップと、を備え、前記ROM領域に記憶された前記第1の暗号鍵および前記第1の識別情報は、作動が停止しても情報が保持される構成を有している。

この構成により、被暗号化暗号鍵を復号するための第2の暗号鍵がROM領域に記憶されているため、車載装置から暗号鍵を取得して電子鍵を偽造することを困難にすることが可能であると共に、暗号化した暗号鍵を記憶し、それを復号化して使用する機能または処理を従来の装置に付加するものであるため、新たに付加するハードウェアやソフトウェア等を最小限に抑えることができるため、安価に安全性を飛躍的に向上させることが可能な認証方法を実現することができる。

#### 【0011】

また、本発明の認証方法は、前記第2の識別情報と前記第1の識別情報とを用いて行う処理認証は、前記第2の識別情報と前記第1の識別情報とが一致する場合に認証し、一致しない場合は認証しない構成を有している。

この構成により、暗号化した暗号鍵を記憶し、それを復号化して使用する機能または処理を従来の装置に付加するものであるため、新たに付加するハードウェアやソフトウェア等を最小限に抑えることができるため、安価に安全性を飛躍的に向上させることが可能であると共に、識別情報間の一致を認証の判断基準とするため、簡易なソフトウェアで構成することが可能な認証方法を実現することができる。

#### 【0012】

##### 【発明の実施の形態】

以下、本発明の実施の形態について、図面を用いて説明する。

##### （第1の実施の形態）

図1は、本発明の一実施の形態に係る車載電子鍵装置のブロック構成を示す図である。図1において、車載電子鍵装置100は、暗号化および復号化の処理を含む信号処理を行う演算処理部（以下、CPU（Central Processing Unit）という。）110、暗号鍵を記憶する不揮発性メモリ（EEPROM（Electrically Erasable Programmable Read-Only Memory）を含む。以下、EEPROMともいい、図1および図2にEEPROMと記す。）120、外部の電子鍵200と無線で通信を行うための無線通信インタフェース130、およびCPU110と不揮発性メモリ120または無線通信インタフェース130とを接続するバス140、150を含むように構成される。

#### 【0013】

CPU110はROM領域111とRAM領域112を有し、CPU110のROM領域111と不揮発性メモリ120の記憶領域121とには、それぞれ暗号鍵が記憶されている。図2を用いてCPU110のROM領域111と不揮発性メモリ120の記憶領域121に記憶されている暗号鍵について説明する。不揮発性メモリ120の記憶領域121には、第1の暗号鍵を暗号化して得られる情報が記憶されている。以下、第1の暗号鍵を暗号化して得られる情報を被暗号化暗号鍵（図2または図3に暗号鍵1'と記す。）という。

#### 【0014】

一方、CPU110のROM領域111には、被暗号化暗号鍵（図2または図3に暗号鍵1'と記す。）を復号化するために用いられる第2の暗号鍵が記憶されている。暗号化装置100が作動すると、CPU110は、不揮発性メモリ120に記憶されている被暗号化暗号鍵（図2または図3に暗号鍵1'と記す。）を読み出し、読み出した被暗号化暗号

鍵（図2または図3に暗号鍵1'と記す。）を復号化して第1の暗号鍵を生成し、自己のRAM領域112に記憶する。CPU110のRAM領域112に記憶された第1の暗号鍵は、CPU110が作動中は保持され、停止すると消失するものである。

#### 【0015】

無線通信インタフェース130は、車載電子鍵装置100が外部の電子鍵200と無線通信し、認証に用いる識別情報（以下、IDという。）を含む情報の送受信を行うようになっている。以下、車載電子鍵装置100が認証に用いるIDを第1のIDという。ここで、第1のIDは、例えばCPU110のROM領域111に記憶させておくのでも良く、送信する情報には、暗号化された第1のIDが含まれ、受信する情報には電子鍵200によって復号化されたIDが含まれるものとする。バス140、150は、CPU110と不揮発性メモリ120または無線通信インタフェース130とを電氣的に接続するものであり、例えばシリアルバスであっても良い。

10

#### 【0016】

ここで、電子鍵200は、上記の第1の暗号鍵を記憶し、暗号化装置100と無線通信する機能、および無線通信インタフェース130経由で送信された情報の復号化を行う機能を有するものとする。そして、電子鍵200は、無線通信インタフェース130経由で送信された情報を復号化して得た情報（以下、第2のIDという。）を暗号化装置100に送信するようになっているものとする。

#### 【0017】

以下に、本発明の第1の実施の形態に係る車載電子鍵装置の動作について図面を用いて説明する。

20

図3は、本発明の第1の実施の形態に係る車載電子鍵装置における処理の流れを示すフローチャートである。

まず、被暗号化暗号鍵（図2または図3に暗号鍵1'と記す。）が不揮発性メモリ（EEPROM）120からCPU110によって読み出され（S310）、第2の暗号鍵がCPU110のROM領域111から読み出される（S320）。

#### 【0018】

次に、ステップS310で読み出された被暗号化暗号鍵（図2または図3に暗号鍵1'と記す。）がステップS320で読み出された第2の暗号鍵を用いて復号化されて第1の暗号鍵が生成され、CPU110のRAM領域112に書き込まれる（S330）。第1の暗号鍵がCPU110のRAM領域112に書き込まれると、認証に用いられるIDを第1の暗号鍵を用いて暗号化し（S340）、この暗号化されたID（以下、第1のIDという。）を無線通信インタフェース130経由で電子鍵200に送信する（S350）。

30

#### 【0019】

ステップS350で第1のIDが電子鍵200に送信されたら、電子鍵200は、第1のIDを受信し、受信した第1のIDを自己が記憶する暗号鍵を用いて復号化して第2のIDを生成し、第2のIDを車載電子鍵装置100に送信するものとする。ここで、車載電子鍵装置100と電子鍵200とは、同一の復号化のアルゴリズムを用い、車載電子鍵装置100によって生成された第1の暗号鍵と電子鍵200が記憶する暗号鍵とが一致する場合、復号化によって得られた第1のIDと第2のIDとは一致し、異なる場合、第1のIDと第2のIDとは一致するようになっている。

40

#### 【0020】

ステップS350で第1のIDを電子鍵200に送信したら、電子鍵200から第2のIDが送信されるのを待ち、送信されたら第2のIDを受信する（S360）。そして、暗号化装置100が保持する第1のIDと受信した第2のIDとを比較して認証を行う（S370）。認証は、第1のIDと第2のIDとが一致するか否かを判断することによって行う。言うまでもなく、両者が一致する場合は認証し、そうでない場合は認証しないようになっている。

#### 【0021】

以上説明したように、本発明の一実施の形態に係る車載電子鍵装置または認証方法は、暗

50

号化されて不揮発性メモリに記憶された第一の暗号鍵をたとえ不揮発性メモリを取り外して読み出しても、これを復号化しない限り使用することはできないため、暗号鍵を取得して電子鍵を偽造することを困難にすることができる。

また、暗号化した暗号鍵を記憶し、それを復号化して使用する機能または処理を従来の装置に付加するものであるため、新たに付加するハードウェアやソフトウェア等を最小限に抑えることができるため、安価に安全性を飛躍的に向上させることができる。

#### 【0022】

#### 【発明の効果】

以上説明したように、本発明は、車載装置から暗号鍵を取得して電子鍵を偽造することを困難にするための車載電子鍵装置および認証方法を実現することができる。

10

#### 【図面の簡単な説明】

【図1】本発明の一実施の形態に係る車載電子鍵装置のブロック構成を示す図

【図2】本発明の一実施の形態に係る車載電子鍵装置において記憶される暗号鍵の記憶場所について説明するための図

【図3】本発明の一実施の形態に係る認証方法における処理の流れを示すフローチャート

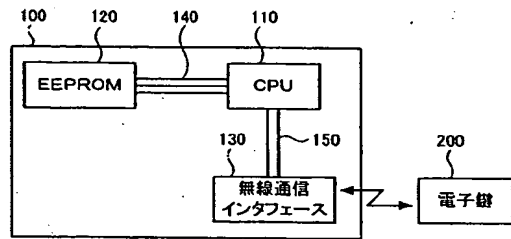
【図4】従来の認証方法における処理の流れを示すフローチャート

#### 【符号の説明】

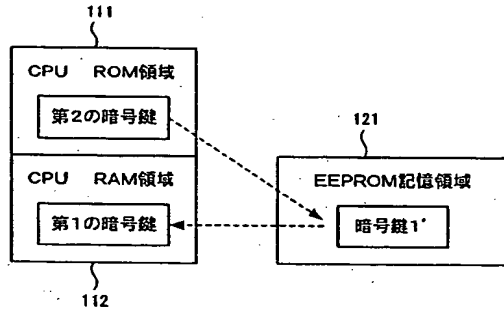
- 100 車載電子鍵装置
- 110 演算処理部 (CPU)
- 111 CPUのROM領域 111
- 112 CPUのRAM領域 112
- 120 不揮発性メモリ
- 121 不揮発性メモリの記憶領域 121
- 130 無線通信インタフェース
- 140、150 バス
- 200 電子鍵

20

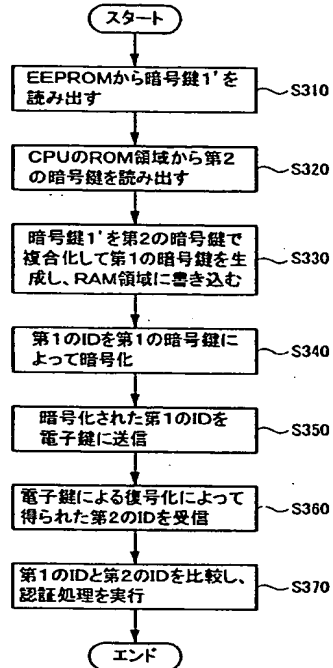
【図 1】



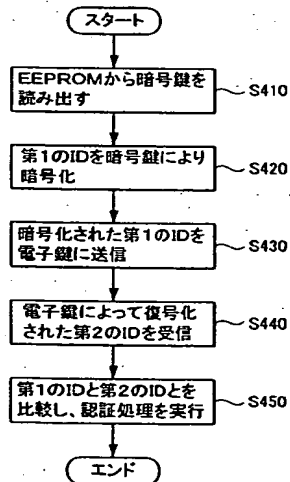
【図 2】



【図 3】



【図 4】





---

フロントページの続き

(51)Int.Cl.<sup>7</sup>

H04L 9/32

F I

H04L 9/00 673C

テーマコード (参考)